IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

JESSICA EMERY, individually and on behalf of all others similarly situated, Plaintiff, v. NEXTGEN HEALTHCARE, INC., Defendant.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Jessica Emery brings this Class Action Complaint on behalf of herself, and all others similarly situated, against Defendant NextGen Healthcare, Inc. ("NextGen" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge:

NATURE OF THE ACTION

1. Business associates of healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. NextGen is a Georgia-based software and services company that provides software and related support to ambulatory healthcare providers ("Customer Healthcare-Providers"), "including practice management, revenue cycle management, patient experience, value-based care, analytics & reporting, and data platforms."[1]

4. As the business associate of its Customer Healthcare-Providers, NextGen knowingly obtains sensitive patient PII and PHI and has a resulting duty to securely maintain such information in confidence and maintain such information

[1] *NextGen Healthcare, Inc. Reports Data Breach Affecting Thousands of Individuals' Social Security Numbers*, JDSupra (May 1, 2023), https://www.jdsupra.com/legalnews/nextgen-healthcare-inc-reports-data-7912620/.

against unauthorized access and disclosure through reasonable and adequate data security measures.

5. On April 28, 2023, Nextgen notified the patients of its Customer-Healthcare providers that their PII and PHI stored on Defendant's NextGen Office System, a cloud-based electronic health records ("EHR") and practice management solution had been accessed by unauthorized third-party (the Data Breach").[2]

6. Based on the public statements of NextGen to date, a wide variety of PII and PHI was implicated in the Data Breach, including but not limited to patient names, dates of birth, addresses, and Social Security numbers.[3]

7. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

8. Plaintiff, on behalf herself, and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks

---

[2] JDSupra, *supra* note 1; Carly Page, *NextGen Healthcare says hackers accessed personal data of more than 1 million patients*, TechCrunch (May 8, 2023), https://techcrunch.com/2023/05/08/nextgen-healthcare-data-breach/.

[3] JDSupra, *supra* note 1.

damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

9. Plaintiff Jessica Emery is an adult, who at all relevant times, is a resident and citizen of the State of North Carolina. Plaintiff was a patient of one of NextGen's Customer-Healthcare Providers. Plaintiff received a Data Breach Notification informing her that her PII and PHI in NextGen's possession had been exposed during the Data Breach.

10. Since the announcement of the Data Breach, Plaintiff has been required to spend her valuable time changing her passwords to her financial and medical accounts to prevent any misuses of her PII and PHI—time which she would not have had to expend but for the Data Breach. Plaintiff has also received a significant increase in spam calls since the announcement of the Data Breach. This was a considerable increase from the amount of spam calls she received prior to the Data Breach.

11. As a result of the Data Breach, Plaintiff will continue to be at a heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

12. Defendant NextGen is a Delaware corporation with a principal place of business located at 3525 Piedmont Road NE, Building 6, Suite 700, Atlanta, Georgia 30305.

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

14. This Court has personal jurisdiction over Defendant because Defendant resides in this District, and at all relevant times, Defendant has engaged in substantial business activities in Georgia.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2), because Defendant resides in this District, and a substantial part of the acts, omissions, and events giving to the claims occurred in this District.

FACTUAL BACKGROUND

A. NextGen and the Services it Provides.

16. NextGen is a provider of EHR and practice management solutions to doctors and ambulatory care providers.[4]

17. Upon information and belief, when administering its EHR and practice management solutions to its Customer-Healthcare Providers, NextGen receives, maintains, and handles PII and PHI from its Customer-Healthcare Providers, which includes patient names, dates of birth, addresses, and Social Security numbers.

18. Upon information and belief, because NextGen receives, maintains, and handles PII and PHI from its Customer-Healthcare Providers, Defendant qualifies as a business associate within the meaning of 45 C.F.R. § 160.103(3) and has therefore entered into Business Associate Agreements with its Customer-Healthcare Providers, becoming a custodian of patient PHI.

19. As a business associate of its Customer-Healthcare Providers, NextGen is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq*.

20. Plaintiff and Class Members directly or indirectly entrusted NextGen with their sensitive and confidential PII and PHI and therefore reasonably expected

[4] *NextGen Healthcare Reports Breach Affecting More than 1 Million Patients*, HIPAA Journal (May 9, 2023), https://www.hipaajournal.com/nextgen-healthcare-reports-breach-affecting-more-than-1-million-patients/.

that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

21. As a custodian of Plaintiff's and Class Members' PII and PHI, NextGen assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

22. Despite NextGen's duty to safeguard the PII and PHI of its Customer-Healthcare Providers' patients, Defendant nevertheless employed inadequate data security measures to protect and secure the PII and PHI entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI.

B. NextGen Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims.

23. NextGen was well aware that the PHI and PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

24. NextGen also knew that a breach of its computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

25. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

26. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[5] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

27. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[6]

28. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[7]

---

[5] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[6] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[7] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20, (last visited Apr. 25, 2023).

29. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[8] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[9]

30. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[10]

31. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the

---

[8] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/, (last visited May 17, 2023).

[9] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names.

[10] *Id.*

information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[11]

32. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[12]

33. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[13]

34. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than

---

[11] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/, (last visited May 2, 2023).

[12] *Id.*

[13] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report, (last visited May 2, 2023).

5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[14]

35. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves the patients of NextGen's Customer-Healthcare Providers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

36. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

37. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle

[14] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

> agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[15]

38. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

39. In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long

[15] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[16]

40. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[17]

---

[16] *Id.*

[17] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

41. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[18]

42. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

43. Based on the value of PII and PHI to cybercriminals, NextGen knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached.

---

[18] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf, (last visited May 2, 2023).

NextGen failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

C. NextGen Demonstrates a Reckless Disregard for Data Security.

44. As the business associate of Customer-Healthcare Providers who collects, maintains, and stores the PII and PHI of countless individuals, NextGen has an obligation to securely maintain the highly sensitive information that it receives and keep it safe from harm. NextGen knows that PII and PHI is a prime target for cybercriminals. Yet, NextGen has major security problems that pose a threat to patients' PII and PHI.

45. In January 2023, NextGen suffered a ransomware attack at the hands of the BlackCat (also known as ALPHV) ransomware group.[19]

46. During the ransomware attack, BlackCat was able to exfiltrate employee information, including names, addresses, phone numbers, and passport scans.[20] The exfiltrated information was later listed on BlackCat's leak site.[21]

---

[19] Tim Starks, *The latest cyberattack on health care shows how vulnerable the sector is*, Wash. Post (Jan. 23, 2023), https://www.washingtonpost.com/politics/2023/01/23/latest-cyberattack-health-care-shows-how-vulnerable-sector-is/.

[20] Page, *supra* note 2.

[21] *Id.*

47. Despite suffering a ransomware attack in January 2023, NextGen suffered a second data breach less than three months later, this time compromising patient PII and PHI.

D. NextGen Breached its Duty to Protected PII and PHI.

48. On or about April 28, 2023, NextGen began notifying patients about a hacking incident that exposed their PII and PHI.[22]

49. According to Defendant, Nextgen was alerted to suspicious activity on its NextGen Office System on March 30, 2023.[23] In response to the discovery, NextGen launched an investigation with the help-of third-party forensics experts.[24]

50. Based on NextGen's investigation, Defendant confirmed that between March 29, 2023, and April 14, 2023, unknown third parties gained unauthorized access to a set of files containing electronically stored personal information.[25] As such, an unknown third-party had unauthorized access to NextGen's computer systems for approximately fourteen days after Defendant first discovered the Data Breach.[26]

---

22 Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml, (last visited May 17, 2023).

23 JDSupra, *supra* note 1.

24 *Id.*

25 *Id.*

26 *Id.*

51. Upon determining that the unknown third-party accessed sensitive personal information, NextGen reviewed the affected files to determine what information was compromised and who was impacted.[27]

52. According to NextGen, the information compromised in the Data Breach includes, *inter alia*, patient names, dates of birth, addresses, and Social Security numbers. [28]

53. On or about April 28, 2023, NextGen filed a notice of the Data Breach with the Office of the Maine Attorney General, indicating that the Data Breach impacted over 1 million individuals.[29] To date, NextGen still has not reported the Data Breach to the United States Department of Health and Human services Office for Civil Rights.

54. On or about the time Defendant notified the Office of the Maine Attorney General, Plaintiff received a Data Breach notice, informing her that her PII and PHI had been exposed during the Data Breach.

55. Upon information and belief, Class Members Received Data Breach notices around that time, also informing them that their PII and/or PHI in NextGen's possession had been exposed during the Data Breach.

---

27 *Id.*

28 *Id.*

29 Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml, (last visited May 17, 2023).

56. The Data Breach occurred as a direct and proximate result of NextGen's failure to implement and follow basic security procedures in order to protect patient PII and PHI.

E. NextGen is Obligated Under HIPAA to Safeguard Personal Information.

57. NextGen is required by the HIPAA to safeguard patient PHI.

58. NextGen is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

59. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

60. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media;" "[m]aintained in electronic media;" or "[t]ransmitted or maintained in any other form or medium."

61. Under C.F.R. 45 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;"

and (3) either (a) "identifies the individual;" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

62. HIPAA requires NextGen to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

63. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers and their business associates to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

64. As such, NextGen is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it acquires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

65. Given the application of HIPAA to NextGen, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to NextGen in order to receive healthcare services from Defendant's Customer-Healthcare Providers,

Plaintiff and Class Members reasonably expected that NextGen would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit NextGen from Engaging in Unfair or Deceptive Acts or Practices.

66. NextGen is prohibited by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

67. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

68. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on

[30] *Start with Security – A Guide for Business*, U.S. FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf, (last visited on May 17, 2023).

networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[31]

69. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. NextGen failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

---

[31] *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, (last visited on May 17, 2023).

[32] *Id*.

72. NextGen was at all times fully aware of its obligations to protect the PII and PHI of its Customer-Healthcare Providers' patients because of its position as a business associate, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Plaintiff and Class Members Suffered Damages.

73. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff, and members of the Class, significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

74. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

75. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

76. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[33]

77. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[34]

78. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[35]

---

[33] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4 (Mar. 7, 2023), https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

[34] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTH IT SEC. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[35] *Id*.

79. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[36]

80. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[37]

81. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[38]

82. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

---

[36] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[37] *Id*.

[38] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

83. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII and/or PHI was compromised in the NextGen Data Breach announced on or about April 28, 2023 (the "Class").

85. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

86. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

87. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there is at a minimum, one million members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable

through NextGen's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately one million individuals.

88. **Commonality:** This action involves questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

89. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. NextGen was the custodian of Plaintiff's and Class Members' PII and PHI, when their PII and PHI was obtained by an unauthorized third party.

90. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

91. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

92. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages

is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

93. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

94. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through NextGen's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

95. Plaintiff restates and realleges paragraphs 1 through 94 above as if fully set forth herein.

96. NextGen owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

97. NextGen duty to use reasonable care arose from several sources, including but not limited to those described below.

98. NextGen had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, NextGen was obligated to act with reasonable care to protect against these foreseeable threats.

99. NextGen's duty also arose from Defendant's position as a business associate. NextGen holds itself out as a trusted business associate of healthcare providers, and thereby assumes a duty to reasonably protect the information it obtains from its Customer-Healthcare Providers. Indeed, NextGen, which receives, maintains, and handles PII and PHI from its Customer-Healthcare Providers, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

100. NextGen breached the duties owed to Plaintiff and Class Members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Nextgen breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in

the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

101. But for NextGen's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

102. As a direct and proximate result of NextGen's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to NextGen with the mutual understanding that NextGen would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in NextGen's possession and is

subject to further breaches so long as NextGen fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

103. As a direct and proximate result of NextGen's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE CLASS)

104. Plaintiff restates and realleges paragraphs 1 through 94 above as if fully set forth herein.

105. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as NextGen or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of NextGen's duty.

106. NextGen violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. NextGen 's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving patient PII and PHI obtained from its Customer-Healthcare Providers.

107. NextGen's violation of Section 5 of the FTC Act constitutes negligence *per se*.

108. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

109. NextGen is an entity covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

110. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, NextGen had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

111. Specifically, HIPAA required NextGen to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the

PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

112. NextGen violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

113. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of NextGen's Customer-Healthcare Providers.

114. NextGen's violation of HIPAA constitutes negligence *per se*.

115. The harm that has occurred as a result of NextGen's conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

116. As a direct and proximate result of NextGen's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to NextGen with the mutual understanding that NextGen would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in NextGen's possession and is

subject to further breaches so long as NextGen fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

117. As a direct and proximate result of NextGen's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

118. Plaintiff restates and realleges paragraphs 1 through 94 above as if fully set forth herein.

119. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

120. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether NextGen is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that NextGen's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and/or PHI will occur in the future.

121. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. NextGen owes a legal duty to secure patient PII and PHI obtained from its Customer-Healthcare Providers and to timely notify such patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA.

b. NextGen breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

122. This Court also should issue corresponding prospective injunctive relief requiring NextGen to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

123. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at NextGen. The risk of another such breach is real, immediate, and substantial. If another breach at NextGen occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

124. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to NextGen if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to NextGen of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and NextGen has a pre-existing legal obligation to employ such measures.

125. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at NextGen, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: May 17, 2023

Respectfully Submitted,

/s/ Nicholas A. Colella

Gary F. Lynch
Nicholas A. Colella
LYNCH CARPENTER, LLP
1133 Penn Ave., Fl. 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
nickc@lcllp.com

Counsel for Plaintiff